

### **REMARKS**

Claims 1-17 are currently pending in the application; with claims 1, 9, and 13 being independent. Applicants have amended claims 1 and 9 to better define the claimed invention; amended claim 3 to address a minor informality; and have amended claim 13 to overcome a §112, second paragraph, rejection.

Applicants respectfully request entry of this amendment and favorable consideration thereof in light of the comments and amendments contained herein, and earnestly seek timely allowance of the pending claims.

#### ***Allowable Subject Matter***

In the outstanding Office Action, the Examiner indicated that claims 6 and 14-16 are directed to allowable subject matter but are objected to as being dependent from a rejected base claim. Applicants wish to thank the Examiner for the indication of allowable subject matter.

#### ***Claim Rejections – 35 USC §112, First Paragraph***

The Office Action indicated that claims 1 and 2 are rejected under 35 USC §112, first paragraph, “because these claims while reciting the location and purpose of an illegal access data handling apparatus, but fail to specify the scope of an apparatus what is composed of. Moreover, it is not clear whether an apparatus or method steps being claimed.” (See Office Action, page 3, second paragraph.) Applicants respectfully traverse the §112, first paragraph, rejection and submit that the basis for the rejection is wholly inappropriate. One of ordinary skill in the art would appreciate that an apparatus is being claimed by inspection of the preamble of claim 1. Additionally, Applicants submit that the Examiner appears to be providing the basis for a §112, second paragraph, rejection because the claim is not clear, which Applicants also do not agree with. In no way acquiescent to the Examiner’s rejection, Applicants have amended claim 1 to better define the claimed invention, and to advance the prosecution of the application.

Accordingly, Applicants respectfully request the Examiner withdraw the §112, first paragraph, rejection of claims 1 and 2.

***Claim Rejections – 35 USC §112, Second Paragraph***

The Examiner indicated that claims 1 and 2 are rejected under 35 USC §112, second paragraph, as being indefinite. Specifically, the Examiner indicated that claims 1 and 2 “provide for the location and purposed of an illegal access data handling apparatus, but do not set forth a method steps or an apparatus claims.” (See Office Action page 3, 3<sup>rd</sup> paragraph.)

Applicants respectfully traverse the Examiner’s rejection and submit that one of ordinary skill in the art would be able to ascertain the metes and bounds of claims 1 and 2. While Applicants do not agree with the Examiner’s rejection, claim 1 has been amended to more appropriate define the present invention and to advance the prosecution of the application.

Regarding claim 13, Applicants have amended this claim in order to address the lack of antecedent basis for “the network device.”

Accordingly, Applicants respectfully request the Examiner to withdraw the §112, second paragraph rejection of claims 1, 2, and 13.

***Claim Rejections – 35 USC §102***

The Examiner rejected claims 1-3 and 9-11 under 35 USC §102(e) as being anticipated by Rothermel. Applicants submit the Examiner has failed to establish a *prima facie* case of anticipation and traverse this rejection.

Regarding claims 1 and 9, Rothermel fails to disclose, at least, “taking countermeasures against the illegal access data received, wherein the countermeasures include providing a response pretending to originate from the internal communications network,” as recited in claim 1, and “taking countermeasures against the illegal access data received, wherein the

countermeasures include providing a response pretending to originate from the internal communications network,” as recited in claim 9.

Rothermel merely discloses a way to remotely manage multiple network security devices. Rothermel further discloses utilizing network security devices (NSD), which attempt to control the spread of sensitive information so only authorized users or devices can retrieve such information. Such types of NSDs, such as firewalls and security appliances, have a group of one or more trusted network devices which the NSD attempts to protect from unauthorized external access (column 1, lines 23-30). The NSD monitors network information passing between external network devices and the devices in their group of trusted internal devices (column 1, lines 30-33). As shown in Fig. 1, the network security device management system includes a security policy manager device 110 able to communicate with multiple superior devices 120 and 160, also referred to as host devices. Each supervisor device is associated with multiple NSDs, with supervisor device 120 associated with NSDs 130-140, and with supervisor device 160 associated with NSDs 161-162. Each NSD protects one or more trusted devices from external devices, such as NSDs 130 and 140 protecting devices in internal networks 135 and 145, respectively, from devices external to network 190.

Rothermel is distinguished by the above-quoted features in that Rothermel is primarily concerned with permitting a network manager to manage multiple NSDs and change their respective security policies utilizing a network security device management system. That is, Rothermel is directed at managing multiple NSDs across an entire network, and fails to disclose providing a response pretending to originate from an internal communications network.

Accordingly, Applicants respectfully request the Examiner to withdraw the rejection to independent claims 1 and 9. Claims 2-8 depend from claim 1 and are allowable at least for the reasons provided above for allowable claim 1; and claims 10-12 depend from claim 9 and are at least allowable for the reasons provided above for allowable claim 9.

***Claim Rejections – 35 USC §103***

The Examiner rejected claims 4, 7, 8, 13, and 17 under 35 USC §103(a) as being unpatentable over Rothermel in view of US Patent No. 6,321,337 to Reshef et al. (“Reshef”). Applicants submit the Examiner has failed to establish a *prima facie* case of obviousness and traverse this rejection.

As mentioned above, Rothermel merely teaches a way to remotely manage multiple security devices (NSD). The NSDs attempt to control the spread of sensitive information so only authorized users or devices can retrieve such information. The NSDs include firewalls and security appliances, which have a group of one or more trusted network devices, which the NSDs attempt to protect from unauthorized external access (column 1, lines 23-30).

However, as the Examiner admits, Rothermel fails to teach or suggest, at least, “encapsulating a response packet so that it appears to originate from the target server,” as recited in claim 13 (emphasis added).

Reshef fails to cure the deficiencies of Rothermel in this respect. Reshef merely discloses methods and systems directed to providing protection to trusted, internal networks from external attacks and the intentional or inadvertent introduction of bugs or viruses (column 1, lines 16-22). Reshef further teaches that separation of the client and server within a bastion server can be enhanced by disabling the forwarding of incoming messages using their native protocol. This prevents exploitation of the operating system by “IP in IP” encapsulation, for example, which sends TCP/IP packets as data inside an outer TCP/IP wrapper. The removing the TCP/IP wrapper would leave a potentially mischievous TCP/IP packet intact. Disabling all TCP/IP forwarding assures that the message forwarded is in a format different from its native TCP/IP format. Barricaded operating systems are further hardened by stripping away all but a severely limited set of functions, so that the processors respond to incoming messages only as daemons.

Reshef further discloses systems to allow users to specify a simplified set of representations of content data which is allowed to pass from an external computing environment to an internal computing environment, and to prevent any content data other than the specified data to pass to the internal environment by converting all allowable data into the simplified representations. This is accomplished by a security gateway positioned between an external, untrusted computing environment and an internal, trusted computing environment that converts messages received from the external environment into simplified messages and converts the simplified messages into messages suitable for use on the internal environment. The conversion involves the removal of external environment transfer protocols and the reduction of the content of the messages left after removing the protocols into a simplified representation of the content to create a simplified message (column 3, line 53 through column 4, line 5).

Reshef is distinguished by the following invention in that Reshef merely discloses encapsulation and decapsulation of TCP/IP into a CIP format (see column 11, lines 44-65). Reshef fails to teach or suggest “encapsulating the response packet so that it appears to originate from the target server,” as recited in claim 13.


Accordingly, Applicants respectfully request the Examiner to withdraw the rejection of claim 13. Claims 14-17 depend from claim 13 and are allowable at least for the reasons provided above for allowable claim 13.

### *Conclusion*

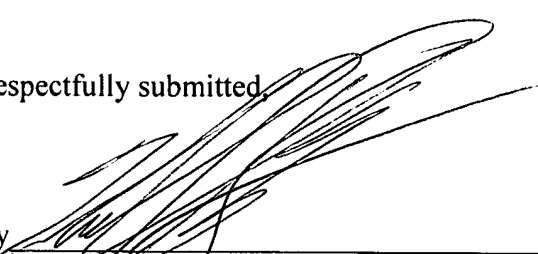
In view of the above amendments and remarks, this application appears to be in condition for allowance and the Examiner is, therefore, requested to reexamine the application and pass the claims to issue.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned at telephone number (703) 205-8000, which is located in the Washington, DC area.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

  
Date: May 2, 2006

Respectfully submitted,

  
By \_\_\_\_\_  
Michael K. Mutter  
Registration No.: 29,680  
BIRCH, STEWART, KOLASCH & BIRCH, LLP  
8110 Gatehouse Rd  
Suite 100 East  
P.O. Box 747  
Falls Church, Virginia 22040-0747  
(703) 205-8000  
Attorney for Applicant